Uniform Distribution Theory **6** (2011), no.1, 185–200

uniform
distribution
theory

CONSTRUCTIONS OF UNIFORMLY DISTRIBUTED SEQUENCES USING THE b-ADIC METHOD

Peter Hellekalek — Harald Niederreiter

ABSTRACT. For bases $\mathbf{b} = (b_1, \ldots, b_s)$ of not necessarily distinct integers $b_i \geq 2$, we employ $\mathbf{b}$-adic arithmetic to study questions in the theory of uniform distribution. A $\mathbf{b}$-adic function system is constructed and the related Weyl criterion is proved. Relations between the uniform distribution of a sequence in the $\mathbf{b}$-adic integers, on the s-dimensional torus, and in the rational integers are established and several constructions of uniformly distributed sequences based on $\mathbf{b}$-adic arithmetic are presented.

Communicated by Henri Faure

1. Introduction

In this paper we present tools for the analysis and for the construction of sequences that are uniformly distributed in the s-dimensional unit cube $[0,1)^s$. Our approach is based on b-adic arithmetic, which means that we employ structural properties of the compact group of b-adic integers.

Any construction method for finite or infinite sequences of points in $[0,1)^s$ will have to employ some arithmetical operations like addition or multiplication, on a suitable domain. It is most helpful if the algebraic structure underlying these operations is an abelian group. The choice of this group determines which function systems will be suitable for the analysis of the equidistribution behavior of this sequence, because the construction method is intrinsically related to the function system, via the concept of the *dual group* (see Hewitt and Ross [6]). An example of such a suitable 'match' between sequences and function systems is given by Kronecker sequences or, in the discrete version, good lattice points, and the trigonometric functions. This construction method is based on *addition*

2010 Mathematics Subject Classification: Primary: 11K06; Secondary: 11K31, 11K41, 11K70, 11L03.
Keywords: uniform distribution of sequences, Weyl criterion, b-adic integers, b-adic function systems, Halton sequence, Fibonacci sequence.

modulo one (see Niederreiter [14, Ch. 5] and Sloan and Joe [16]). A second example is digital nets and sequences and the Walsh functions. Here, *addition without carry* of digit vectors comes into play (see Niederreiter [14, Ch. 4] and Dick and Pillichshammer [2] for details).

One important type of a digital sequence, the Halton sequence, can also be generated by *addition with carry* of digit vectors, the underlying group being the compact group of b-adic integers. This observation is the starting point for this paper.

In Section 2, we extend results of the first author [4, 5] from the case of prime bases to arbitrary bases $\mathbf{b} = (b_1, \ldots, b_s)$ with not necessarily distinct integers $b_i \geq 2$. We show that the associated $\mathbf{b}$-adic function system is an orthonormal basis of the Hilbert space $L^2([0,1)^s)$ and we prove the $\mathbf{b}$-adic Weyl criterion, among other results.

In Section 3 we review results on the uniform distribution of integer lattice points modulo vectors $\mathbf{m} = (m_1, \ldots, m_s)$ of positive integers. As an application, in Section 4 criteria for the uniform distribution of sequences of rationals in $[0,1)^s$ are established that relate the $\mathbf{b}$-adic approach to uniform distribution of lattice points.

In Section 5 various types of sequences and their uniform distribution are discussed.

2. The b-adic function system on $[0,1)^s$

In this section, we will extend the concept of $\mathbf{p}$-adic function systems introduced in [4, 5] from the case of prime bases to general bases. The cornerstones of this approach are the enumeration of the dual group of the compact group of $\mathbf{b}$-adic integers (see Remark 2.3), the $\mathbf{b}$-adic function system, which is an orthonormal basis of the space $L^2([0,1)^s)$ (Theorem 2.12), and the fact that the indicator functions of particular subintervals of $[0,1)^s$, so-called $\mathbf{b}$-adic elementary intervals, have finite Fourier series (Lemma 2.10), with pointwise identity (Lemma 2.11).

Throughout this paper, b denotes a positive integer, $b \geq 2$, and $\mathbf{b} = (b_1, \ldots, b_s)$ stands for a vector of not necessarily distinct integers $b_i \geq 2$, $1 \leq i \leq s$. $\mathbb{N}$ represents the positive integers, and we put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

The underlying space is the s-dimensional torus $\mathbb{R}^s/\mathbb{Z}^s$, which will be identified with the half-open interval $[0,1)^s$. Haar measure on the s-torus $[0,1)^s$ will be denoted by λ_s. We put $e(y) = \mathrm{e}^{2\pi \mathrm{i} y}$ for $y \in \mathbb{R}$, where i is the imaginary unit.

We will use the standard convention that empty sums have the value 0 and empty products value 1.

For a nonnegative integer k, let $k = \sum_{j\geq 0} k_j\, b^j$, $k_j \in \{0, 1, \ldots, b-1\}$, be the unique b-adic representation of k in base b. With the exception of at most finitely many indices j, the digits k_j are equal to 0.

Every real number $x \in [0,1)$ has a b-adic representation $x = \sum_{j\geq 0} x_j\, b^{-j-1}$, with digits $x_j \in \{0, 1, \ldots, b-1\}$. If x is a *b-adic rational*, which means that $x = ab^{-g}$, a and g integers, $0 \leq a < b^g$, $g \in \mathbb{N}$, and if $x \neq 0$, then there exist two such representations.

The b-adic representation of x is uniquely determined under the condition that $x_j \neq b-1$ for infinitely many j. In the following, we will call this particular representation the *regular* (b-adic) representation of x.

Let $\mathbb{Z}_b$ denote the compact group of the b-adic integers. We refer the reader to Hewitt and Ross [6] and Mahler [10] for details. An element z of $\mathbb{Z}_b$ will be written in the form $z = \sum_{j\geq 0} z_j\, b^j$, with digits $z_j \in \{0, 1, \ldots, b-1\}$.

The set $\mathbb{Z}$ of integers is embedded in $\mathbb{Z}_b$. If $z \in \mathbb{N}_0$, then at most finitely many digits z_j are different from 0. If $z \in \mathbb{Z}$, $z < 0$, then at most finitely many digits z_j are different from $b-1$. In particular, $-1 = \sum_{j\geq 0}(b-1)\, b^j$.

We recall the following concepts from Hellekalek [4, 5].

Definition 2.1. The map $\varphi_b : \mathbb{Z}_b \to [0,1)$, given by

$$\varphi_b\left(\sum_{j\geq 0} z_j\, b^j\right) = \sum_{j\geq 0} z_j\, b^{-j-1} \pmod 1,$$

will be called the *b-adic Monna map*.

The restriction of φ_b to $\mathbb{N}_0$ is often called the *radical-inverse function* in base b. The Monna map is surjective, but not injective. It may be inverted in the following sense.

Definition 2.2. We define the *pseudoinverse* φ_b^+ of the b-adic Monna map φ_b by

$$\varphi_b^+ : [0,1) \to \mathbb{Z}_b, \quad \varphi_b^+\left(\sum_{j\geq 0} x_j\, b^{-j-1}\right) = \sum_{j\geq 0} x_j\, b^j\ ,$$

where

$$\sum_{j\geq 0} x_j\, b^{-j-1}$$

stands for the regular b-adic representation of the element $x \in [0,1)$.

The image of $[0,1)$ under φ_b^+ is the set $\mathbb{Z}_b \setminus (-\mathbb{N})$. Furthermore, $\varphi_b \circ \varphi_b^+$ is the identity map on $[0,1)$, and $\varphi_b^+ \circ \varphi_b$ the identity on $\mathbb{N}_0 \subset \mathbb{Z}_b$. In general, $z \neq \varphi_b^+\big(\varphi_b(z)\big)$, for $z \in \mathbb{Z}_b$. For example, if $z = -1$, then

$$\varphi_b^+\big(\varphi_b(-1)\big) = \varphi_b^+(0) = 0 \neq -1.$$

A central point in the concept of $\mathbf{p}$-adic function systems introduced in [4, 5] is the enumeration of the dual group $\hat{\mathbb{Z}}_p$, p a prime. We extend this approach to general integer bases as follows. In analogy to [8, Sect. 5.2, pp. 322 ff], let R_b denote the set of b-adic rationals in $[0,1)$. Put $R_b(0) = \{0\}$ and, for $g \in \mathbb{N}$, let

$$R_b(g) = \left\{ab^{-g}, 1 \le a < b^g : \ a \in \mathbb{N}, b \not| a\right\}.$$

The set R_b is the disjoint union of the sets $R_b(g)$, taken over all $g \in \mathbb{N}_0$. We refer the reader to [6] for the relation between R_b and the dual group $\hat{\mathbb{Z}}_b$ of $\mathbb{Z}_b$.

Remark 2.3. For every $g \in \mathbb{N}$, the function φ_b gives a bijection between the subset of positive integers $\{k \in \mathbb{N} : b^{g-1} \le k < b^g\}$ and the set $R_b(g)$. As a consequence, $\hat{\mathbb{Z}}_b$ can be written in the form

$$\hat{\mathbb{Z}}_b = \{\chi_k : k \in \mathbb{N}_0\},$$

where

$$\chi_k : \mathbb{Z}_b \to \{c \in \mathbb{C} : |c| = 1\}, \quad \chi_k\left(\sum_{j \ge 0} z_j b^j\right) = e\big(\varphi_b(k)(z_0 + z_1 b + \cdots)\big).$$

We note that χ_k depends only on a finite number of digits of z and, hence, this function is well defined.

As in [5], we employ the function φ_b^+ to lift the characters χ_k to the torus.

Definition 2.4. For $k \in \mathbb{N}_0$, let $\gamma_k : [0,1) \to \{c \in \mathbb{C} : |c| = 1\}$, $\gamma_k(x) = \chi_k\big(\varphi_b^+(x)\big)$, denote the kth b-adic function. We put $\Gamma_b = \{\gamma_k : k \in \mathbb{N}_0\}$ and call it the b-adic function system on $[0,1)$.

There is an obvious generalization of the preceding notions to the higher-dimensional case. Let $\mathbf{b} = (b_1, \ldots, b_s)$ be a vector of not necessarily distinct integers $b_i \ge 2$, let $\mathbf{x} = (x_1, \ldots, x_s) \in [0,1)^s$, let $\mathbf{z} = (z_1, \ldots, z_s)$ denote an element of the compact product group $\mathbb{Z}_{\mathbf{b}} = \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{b_s}$ of $\mathbf{b}$-adic integers, and let $\mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$. We define $\varphi_{\mathbf{b}}(\mathbf{z}) = \big(\varphi_{b_1}(z_1), \ldots, \varphi_{b_s}(z_s)\big)$, and $\varphi_{\mathbf{b}}^+(\mathbf{x}) = \big(\varphi_{b_1}^+(x_1), \ldots, \varphi_{b_s}^+(x_s)\big)$.

Let $\chi_{\mathbf{k}}(\mathbf{z}) = \prod_{i=1}^s \chi_{k_i}(z_i)$, where $\chi_{k_i} \in \hat{\mathbb{Z}}_{b_i}$, and define $\gamma_{\mathbf{k}}(\mathbf{x}) = \prod_{i=1}^s \gamma_{k_i}(x_i)$, where $\gamma_{k_i} \in \Gamma_{b_i}$, $1 \le i \le s$. Then $\gamma_{\mathbf{k}} = \chi_{\mathbf{k}} \circ \varphi_{\mathbf{b}}^+$. Let $\Gamma_{\mathbf{b}}^{(s)} = \{\gamma_{\mathbf{k}} : \mathbf{k} \in \mathbb{N}_0^s\}$ denote the $\mathbf{b}$-*adic function system* in dimension s.

The dual group $\hat{\mathbb{Z}}_{\mathbf{b}}$ is an orthonormal basis of the Hilbert space $L^2(\mathbb{Z}_{\mathbf{b}})$. It would follow from some measure-theoretic arguments that $\Gamma_{\mathbf{b}}^{(s)}$ is an orthonormal basis of $L^2([0,1)^s)$. Below, we present a more elementary approach to prove this important property of the $\mathbf{b}$-adic function system. As a side effect, we obtain several helpful insights and results, like the $\mathbf{b}$-adic Weyl criterion.

For an integrable function f on $[0,1)^s$, the $\mathbf{k}$th Fourier coefficient of f with respect to the function system $\Gamma_{\mathbf{b}}^{(s)}$ is defined as the inner product $\langle f, \gamma_{\mathbf{k}} \rangle$ in $L^2([0,1)^s)$:

$$\hat{f}(\mathbf{k}) = \int_{[0,1)^s} f \overline{\gamma_{\mathbf{k}}} \, d\lambda_s, \quad \mathbf{k} \in \mathbb{N}_0^s.$$

We denote the formal Fourier series of f by s_f,

$$s_f = \sum_{\mathbf{k} \in \mathbb{N}_0^s} \hat{f}(\mathbf{k}) \gamma_{\mathbf{k}},$$

where, for the moment, we ignore questions of convergence.

Definition 2.5. A $\mathbf{b}$-*adic elementary interval*, or $\mathbf{b}$-*adic elint* for short, is a subinterval $I_{\mathbf{c},\mathbf{g}}$ of $[0,1)^s$ of the form

$$I_{\mathbf{c},\mathbf{g}} = \prod_{i=1}^{s} \left[\varphi_{b_i}(c_i), \varphi_{b_i}(c_i) + b_i^{-g_i} \right) ,$$

where the parameters are subject to the conditions

$$\mathbf{g} = (g_1, \dots, g_s) \in \mathbb{N}_0^s, \quad \mathbf{c} = (c_1, \dots, c_s) \in \mathbb{N}_0^s, \quad \text{and} \quad 0 \le c_i < b_i^{g_i}, \quad 1 \le i \le s.$$

We say that $I_{\mathbf{c},\mathbf{g}}$ belongs to the resolution class defined by $\mathbf{g}$ or that it has resolution $\mathbf{g}$.

A $\mathbf{b}$-*adic interval* in the resolution class defined by $\mathbf{g} \in \mathbb{N}_0^s$ (or with resolution $\mathbf{g}$) is a subinterval of $[0,1)^s$ of the form

$$\prod_{i=1}^{s} \left[a_i b_i^{-g_i}, d_i b_i^{-g_i} \right), \quad 0 \le a_i < d_i \le b_i^{g_i}, \ a_i, d_i \in \mathbb{N}_0, \ 1 \le i \le s .$$

For a given resolution $\mathbf{g} \in \mathbb{N}_0^s$, we define the following domains:

$$\Delta_{\mathbf{b}}(\mathbf{g}) = \left\{ \mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s : \ 0 \le k_i < b_i^{g_i}, 1 \le i \le s \right\},$$
$$\Delta_{\mathbf{b}}^*(\mathbf{g}) = \Delta_{\mathbf{b}}(\mathbf{g}) \setminus \{\mathbf{0}\} .$$

We note that $\Delta_{\mathbf{b}}(\mathbf{0}) = \{\mathbf{0}\}$.

Remark 2.6. For a given resolution $\mathbf{g} \in \mathbb{N}_0^s$, the family of $\mathbf{b}$-adic elints $\{I_{\mathbf{c},\mathbf{g}} : \mathbf{c} \in \Delta_{\mathbf{b}}(\mathbf{g})\}$ is a partition of $[0,1)^s$.

The following function will allow for a compact notation. For $k \in \mathbb{N}_0$, with b-adic representation $k = k_0 + k_1 b + \cdots$, we define

$$v_b(k) = \begin{cases} 0 & \text{if } k = 0, \\ 1 + \max\{j : k_j \neq 0\} & \text{if } k \geq 1. \end{cases}$$

If $\mathbf{k} \in \mathbb{N}_0^s$, then let $v_{\mathbf{b}}(\mathbf{k}) = \big(v_{b_1}(k_1), \dots, v_{b_s}(k_s)\big)$.

Lemma 2.7. *For every $\mathbf{k} \in \mathbb{N}_0^s$, $\gamma_{\mathbf{k}}$ is a step function given by*

$$\gamma_{\mathbf{k}}(\mathbf{x}) = \sum_{\mathbf{c} \in \Delta_{\mathbf{b}}(v_{\mathbf{b}}(\mathbf{k}))} \chi_{\mathbf{k}}(\mathbf{c}) \mathbf{1}_{I_{\mathbf{c}, v_{\mathbf{b}}(\mathbf{k})}}(\mathbf{x}) \quad \forall \mathbf{x} \in [0,1)^s.$$

Proof. We argue as in the proof of Lemma 3.5 in [5]. □

Corollary 2.8. *For every $\mathbf{k} \neq \mathbf{0}$, the function $\gamma_{\mathbf{k}}$ has integral* 0.

Proof. If $\mathbf{k} \neq \mathbf{0}$, then $\sum_{\mathbf{c} \in \Delta_{\mathbf{b}}(v_{\mathbf{b}}(\mathbf{k}))} \chi_{\mathbf{k}}(\mathbf{c}) = 0$. □

Lemma 2.9. *The class of functions $\Gamma_{\mathbf{b}}^{(s)}$ is an orthonormal system in the space $L^2([0,1)^s)$.*

Proof. It is elementary to verify that the inner product $\langle \gamma_{\mathbf{k}}, \gamma_{\mathbf{k}'} \rangle$ is equal to 0 if $\mathbf{k} \neq \mathbf{k}'$, and equal to 1 if $\mathbf{k} = \mathbf{k}'$. □

A key ingredient in the $\mathbf{b}$-adic approach is the study of the Fourier series of indicator functions $\mathbf{1}_I$ of $\mathbf{b}$-adic elints and intervals I.

Lemma 2.10. *Let $I_{\mathbf{c},\mathbf{g}}$ be an arbitrary $\mathbf{b}$-adic elint. Then*

$$\hat{\mathbf{1}}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{k}) = \begin{cases} 0 & \text{if } \mathbf{k} \notin \Delta_{\mathbf{b}}(\mathbf{g}), \\ \lambda_s(I_{\mathbf{c},\mathbf{g}}) \overline{\chi_{\mathbf{k}}(\mathbf{c})} & \text{if } \mathbf{k} \in \Delta_{\mathbf{b}}(\mathbf{g}). \end{cases}$$

Proof. It is straightforward to adapt the proof of Lemma 3.1 in [4] to the s-dimensional case and to a general base $\mathbf{b}$. □

Lemma 2.11. *Let $I_{\mathbf{c},\mathbf{g}}$ be an arbitrary $\mathbf{b}$-adic elint and put $f = \mathbf{1}_{I_{\mathbf{c},\mathbf{g}}}$. Then $f = s_f$ in the space $L^2([0,1)^s)$ and even pointwise equality holds:*

$$\mathbf{1}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{x}) = \sum_{\mathbf{k} \in \Delta_{\mathbf{b}}(\mathbf{g})} \hat{\mathbf{1}}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{k}) \gamma_{\mathbf{k}}(\mathbf{x}) \quad \forall \mathbf{x} \in [0,1)^s. \tag{1}$$

Proof. The function $f - s_f$ is orthogonal to every function $\gamma_{\mathbf{k}}$. We deduce that

$$\|f - s_f\|_2^2 = \langle f, f\rangle - \langle s_f, f\rangle = \lambda_s(I_{\mathbf{c},\mathbf{g}}) - \prod_{i=1}^{s} b_i^{-g_i} = 0.$$

This implies that $f = s_f$ almost everywhere on $[0,1)^s$.

From Lemma 2.7 it follows that the function s_f is a step function on the same partition $\{I_{\mathbf{d},\mathbf{g}} : \mathbf{d} \in \Delta_{\mathbf{b}}(\mathbf{g})\}$ of $[0,1)^s$ as the function f. As a consequence of equality almost everywhere, f and s_f must coincide on every elint of the partition. Hence, these two step functions are equal in every point of $[0,1)^s$. □

Theorem 2.12. *The function system $\Gamma_{\mathbf{b}}^{(s)}$ is an orthonormal basis of $L^2([0,1)^s)$.*

Proof. The idea of the proof is to show that in the Hilbert space $L^2([0,1)^s)$, the set of finite linear combinations of elements of $\Gamma_{\mathbf{b}}^{(s)}$ is dense in the set of functions $\mathbf{1}_J$, J an arbitrary subinterval of $[0,1)^s$. From this property it follows by a standard argument that $\Gamma_{\mathbf{b}}^{(s)}$ is an orthonormal basis.

Given an arbitrary subinterval J of $[0,1)^s$, it is a straightforward adaption of the method of proof used in [5, Lemma 3.9] to show that J can be approximated arbitrarily closely from within and from without by $\mathbf{b}$-adic intervals $\underline{J}$ and $\overline{J}$, by choosing a suitable resolution $\mathbf{g}$. The latter intervals are finite disjoint unions of $\mathbf{b}$-adic elints. Thus, by Lemma 2.11, the indicator functions $\mathbf{1}_{\underline{J}}$ and $\mathbf{1}_{\overline{J}}$ have finite Fourier series. As a consequence, the function $\mathbf{1}_J$ can be approximated arbitrarily closely in $L^2([0,1)^s)$ by finite linear combinations of functions from $\Gamma_{\mathbf{b}}^{(s)}$. □

Remark 2.13. The method of proof of Lemmas 2.7 - 2.11 and Theorem 2.12 is not limited to the function system $\Gamma_{\mathbf{b}}^{(s)}$. It applies also to the system of Walsh functions in base $\mathbf{b}$, for example. The latter are an obvious generalization of the case $\mathbf{b} = (b, \dots, b)$ to the general case studied in this paper. As a consequence, we obtain a different proof for several pointwise identities for the Fourier series of the indicator functions of elints, like identity (1) in [5, Lemma 3.4] or identity (10) in [3, Theorem 1]. We also obtain a generalization of Theorem A.11 in Dick and Pillichshammer [2, p. 562] and, in addition, a different method of proof.

If $\omega = (\mathbf{x}_n)_{n\geq 0}$ is a -possibly finite- sequence on the torus $[0,1)^s$ with at least N elements, and if $f : [0,1)^s \to \mathbb{C}$, we define

$$S_N(f,\omega) = \frac{1}{N}\sum_{n=0}^{N-1} f(\mathbf{x}_n).$$

Lemma 2.14. *A sequence ω is uniformly distributed in $[0,1)^s$ if and only if*

$$\lim_{N\to\infty} S_N(\mathbf{1}_I,\omega) = \lambda_s(I),$$

for every $\mathbf{b}$*-adic elint I in* $[0,1)^s$.

Proof. We observe that $S_N(\mathbf{1}_I,\omega) - \lambda_s(I) = S_N\big(\mathbf{1}_I - \lambda_s(I),\omega\big)$. It is an easy exercise to translate the proof of Lemma 3.9 in [5] into the case of general bases. □

The notion of a (t,m,s)-net in base b is one of the most important concepts in the modern theory of quasi-Monte Carlo methods and its applications. We refer the reader to Niederreiter [14] and Dick and Pillichshammer [2] for details.

Definition 2.15. For given integers $s \geq 1$, $b \geq 2$, $m \geq 1$, and t, $0 \leq t \leq m$, a finite sequence ω of b^m points in $[0,1)^s$ is called a (t,m,s)-net in base b if $S_{b^m}(\mathbf{1}_{I_{\mathbf{c},\mathbf{g}}},\omega) = \lambda_s(I_{\mathbf{c},\mathbf{g}})$, for all $\mathbf{b}$-adic elints $I_{\mathbf{c},\mathbf{g}}$ where $\mathbf{b} = (b,\dots,b)$ and where the resolution $\mathbf{g}$ satisfies the condition $g_1 + \cdots + g_s \leq m - t$.

We obtain the following characterization of these finite point sets in terms of the system $\Gamma_{\mathbf{b}}^{(s)}$, where $\mathbf{b} = (b,\dots,b)$:

Lemma 2.16. *A sequence $\omega = (\mathbf{x}_n)_{n=0}^{N-1}$ of $N = b^m$ points in $[0,1)^s$ is a (t,m,s)-net in base b if and only if*

$$S_N(\gamma_{\mathbf{k}},\omega) = 0 \quad \forall \mathbf{k} : 0 < \sum_{i=1}^{s} v_b(k_i) \leq m - t. \tag{2}$$

Proof. Put $N = b^m$ and $\mathbf{b} = (b,\dots,b)$. If ω is a (t,m,s)-net in base b, then Lemma 2.7 implies

$$S_N(\gamma_{\mathbf{k}},\omega) = \left(\prod_{i=1}^{s} b^{-v_b(k_i)}\right) \sum_{\mathbf{c}\in\Delta_{\mathbf{b}}(v_{\mathbf{b}}(\mathbf{k}))} \chi_{\mathbf{k}}(\mathbf{c}) = 0$$

for those indices $\mathbf{k}$ such that $0 < v_b(k_1) + \cdots + v_b(k_s) \leq m - t$. This proves (2).

For the reverse direction, assume (2). The pointwise identity in Lemma 2.11 implies that

$$S_N(\mathbf{1}_{I_{\mathbf{c},\mathbf{g}}},\omega) = \hat{\mathbf{1}}_{I_{\mathbf{c},\mathbf{g}}}(\mathbf{0}) = \lambda_s(I_{\mathbf{c},\mathbf{g}})$$

for all $\mathbf{b}$-adic elints with $g_1 + \cdots + g_s \leq m - t$. By definition, ω is a (t,m,s)-net in base b. □

Theorem 2.17 (Weyl criterion for $\Gamma_{\mathbf{b}}^{(s)}$)**.** *Let ω be a sequence in $[0,1)^s$. Then ω is uniformly distributed in $[0,1)^s$ if and only if*

$$\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}},\omega) = 0 \quad \forall\ \mathbf{k} \neq \mathbf{0}. \tag{3}$$

P r o o f. Let ω be uniformly distributed in $[0,1)^s$. Each function $\gamma_{\mathbf{k}}$ is a step function on $[0,1)^s$, hence Riemann integrable. The uniform distribution of ω implies that $S_N(\gamma_{\mathbf{k}},\omega)$ tends to the integral of $\gamma_{\mathbf{k}}$, which is 0 if $\mathbf{k} \neq \mathbf{0}$. This proves (3).

For the reverse direction, let us assume relation (3). In identity (1), the summation domain $\Delta_{\mathbf{b}}(\mathbf{g})$ is finite. Thus, relation (3) implies $\lim_{N\to\infty} S_N(\mathbf{1}_I,\omega) = \lambda_s(I)$, for every $\mathbf{b}$-adic elint I. From Lemma 2.14, the uniform distribution of ω follows. $\square$

Corollary 2.18. *Let $\omega = (\mathbf{x}_n)_{n\geq 0}$, $\mathbf{x}_n = \big(\varphi_{b_1}(n),\dots,\varphi_{b_s}(n)\big)$, be the Halton sequence in base $\mathbf{b} = (b_1,\dots,b_s)$. Then ω is uniformly distributed in $[0,1)^s$ if and only if the bases b_i are pairwise coprime.*

P r o o f. This is easily seen by the Weyl criterion for $\Gamma_{\mathbf{b}}^{(s)}$. If the bases b_i are not pairwise coprime, then it is a simple task to find an index $\mathbf{k} \neq \mathbf{0}$ such that $S_N(\gamma_{\mathbf{k}},\omega) = 1$, for all N. As a consequence, ω is not uniformly distributed in this case.

Let us now suppose that the bases b_i are pairwise coprime. We have

$$\gamma_{\mathbf{k}}(\mathbf{x}_n) = \prod_{i=1}^{s} e\big(\varphi_{b_i}(k_i)n\big) .$$

Hence, for every $\mathbf{k} \neq \mathbf{0}$,

$$\begin{aligned} |S_N(\gamma_{\mathbf{k}},\omega)| &= \frac{1}{N}\left|\frac{e(\varphi_{b_1}(k_1)+\cdots+\varphi_{b_s}(k_s))^N - 1}{e\big(\varphi_{b_1}(k_1)+\cdots+\varphi_{b_s}(k_s)\big) - 1}\right| \\ &\leq \frac{1}{N}\left|\sin\Big(\pi\big(\varphi_{b_1}(k_1)+\cdots+\varphi_{b_s}(k_s)\big)\Big)\right|^{-1}, \end{aligned}$$

where the fact that the bases b_i are pairwise coprime ensures

$$\varphi_{b_1}(k_1)+\cdots+\varphi_{b_s}(k_s) \notin \mathbb{Z}.$$

Hence, $\lim_{N\to\infty} S_N(\gamma_{\mathbf{k}},\omega) = 0$. $\square$

3. Background on uniform distribution in $\mathbb{Z}^s$

We recall some concepts and results from the paper Niederreiter [13] on uniform distribution of sequences of lattice points. Let $s \geq 1$ be a given dimension and let $\mathbf{m} = (m_1,\dots,m_s) \in \mathbb{N}^s$. For $\mathbf{b} = (b_1,\dots,b_s) \in \mathbb{Z}^s$ and $\mathbf{c} = (c_1,\dots,c_s) \in \mathbb{Z}^s$, we write $\mathbf{b} \equiv \mathbf{c} \pmod{\mathbf{m}}$ if $b_i \equiv c_i \pmod{m_i}$ for $1 \leq i \leq s$.

Definition 3.1. The sequence $(\mathbf{y}_n)_{n\geq 0}$ of elements of $\mathbb{Z}^s$ is *uniformly distributed* mod $(m_1,\dots,m_s)$ if

$$\lim_{N\to\infty}\frac{1}{N}\#\{0\leq n<N:\mathbf{y}_n\equiv\mathbf{d}\ (\mathrm{mod}\ \mathbf{m})\}=\frac{1}{m_1\cdots m_s}\qquad\text{for all } \mathbf{d}\in\mathbb{Z}^s.$$

The following Weyl criterion for uniform distribution mod $(m_1,\dots,m_s)$ was stated in Niederreiter [13, Theorem 2.1].

Lemma 3.2. *Let*

$$\mathbf{y}_n=(y_{n1},\dots,y_{ns})\in\mathbb{Z}^s\quad\textit{for}\quad n=0,1,\dots,\qquad\textit{and}\qquad(m_1,\dots,m_s)\in\mathbb{N}^s.$$

Then the sequence $(\mathbf{y}_n)_{n\geq 0}$ *is uniformly distributed modulo* $(m_1,\dots,m_s)$ *if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}e\left(\frac{h_1}{m_1}y_{n1}+\cdots+\frac{h_s}{m_s}y_{ns}\right)=0$$

for all $(h_1,\dots,h_s)\in\mathbb{Z}^s\setminus\{\mathbf{0}\}$ *with* $0\leq h_i<m_i$ *for* $1\leq i\leq s$.

The following result was shown in Niederreiter [13, Theorem 2.5].

Lemma 3.3. *Let*

$$(m_1,\dots,m_s)\in\mathbb{N}^s\quad\textit{and}\quad x_{ni}\in\mathbb{R}\quad\textit{for}\quad n\geq 0\quad\textit{and}\quad 1\leq i\leq s.$$

If the sequence

$$\Big(\big(\{x_{n1}/m_1\},\dots,\{x_{ns}/m_s\}\big)\Big)_{n\geq 0}\quad\textit{is uniformly distributed in } [0,1)^s,$$

then the sequence

$$\Big(\big(\lfloor x_{n1}\rfloor,\dots,\lfloor x_{ns}\rfloor\big)\Big)_{n\geq 0}\quad\textit{is uniformly distributed modulo } (m_1,\dots,m_s).$$

4. Some criteria

Let $s\geq 1$ again be a given dimension. For each $i=1,\dots,s$, let $f_i:\mathbb{N}_0\to\mathbb{N}_0$ be a self-map of $\mathbb{N}_0$. We write $\mathbf{f}=(f_1,\dots,f_s)$, $\mathbf{f}:\mathbb{N}_0\to\mathbb{N}_0^s$.

For arbitrary (not necessarily distinct) integers $b_1,\dots,b_s$, with $b_i\geq 2$, $1\leq i\leq s$, we define the points

$$\mathbf{x}_n=\Big(\varphi_{b_1}\big(f_1(n)\big),\dots,\varphi_{b_s}\big(f_s(n)\big)\Big)\in[0,1)^s,\quad n=0,1,\dots\tag{4}$$

The sequence $(\mathbf{x}_n)_{n\geq 0}$ can be viewed as a generalization of the Halton sequence in base $\mathbf{b}=(b_1,\dots,b_s)$. For a generalization in a different direction, we refer to [7].

We refer the reader to Beer [1] and to Kuipers and Niederreiter [8, Sect. 5.2] for the notion of uniform distribution in the compact group $\mathbb{Z}_p$, p a prime, and to Meijer [11] for the generalization to $\mathbb{Z}_b$.

Definition 4.1. A sequence ω is uniformly distributed in $\mathbb{Z}_b$ if, for all $z \in \mathbb{Z}_b$ and all $g \in \mathbb{N}$,

$$\lim_{N\to\infty} S_N(\mathbf{1}_{z+b^g\mathbb{Z}_b}, \omega) = b^{-g}.$$

This definition is easily extended to the compact product group $\mathbb{Z}_{\mathbf{b}}$, by considering subsets of the form $(z_1 + b_1^{g_1}\mathbb{Z}_{b_1}) \times \cdots \times (z_s + b_s^{g_s}\mathbb{Z}_{b_s})$, where $z_i \in \mathbb{Z}_{b_i}$ and $g_i \in \mathbb{N}$, $1 \le i \le s$.

Theorem 4.2. *The following properties are equivalent:*

(i) *the sequence $(\mathbf{x}_n)_{n\ge0}$ of points in (4) is uniformly distributed in $[0,1)^s$;*

(ii) *the sequence $\big(\mathbf{f}(n)\big)_{n\ge0}$ of elements of $\mathbb{Z}^s$ is uniformly distributed modulo $(b_1^{g_1}, \dots, b_s^{g_s})$ for all $g_1, \dots, g_s \in \mathbb{N}_0$ that are not all 0;*

(iii) *the sequence $\big(\mathbf{f}(n)\big)_{n\ge0}$ is uniformly distributed modulo $(b_1^g, \dots, b_s^g)$ for all $g \in \mathbb{N}$;*

(iv) *the sequence $\big(\mathbf{f}(n)\big)_{n\ge0}$ of elements of $\mathbb{Z}_{\mathbf{b}}$ is uniformly distributed in $\mathbb{Z}_{\mathbf{b}}$.*

Proof. (i) $\Leftrightarrow$ (ii). Let $\omega = (\mathbf{x}_n)_{n\ge0}$ be the sequence of points in (4). By the $\mathbf{b}$-adic Weyl criterion (Theorem 2.17) ω is uniformly distributed in $[0,1)^s$ if and only if $S_N(\gamma_{\mathbf{k}}, \omega)$ tends to 0 if N tends to infinity, for all $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ with $\mathbf{k} \ne \mathbf{0}$. By the definitions of $\gamma_{\mathbf{k}}$ and $\mathbf{x}_n$, we have

$$\begin{aligned} S_N(\gamma_{\mathbf{k}}, \omega) &= \frac{1}{N}\sum_{n=0}^{N-1}\prod_{i=1}^{s}\gamma_{k_i}\Big(\varphi_{b_i}\big(f_i(n)\big)\Big) = \frac{1}{N}\sum_{n=0}^{N-1}\prod_{i=1}^{s}\chi_{k_i}\big(f_i(n)\big) \\ &= \frac{1}{N}\sum_{n=0}^{N-1} e\big(\varphi_{b_1}(k_1)f_1(n) + \cdots + \varphi_{b_s}(k_s)f_s(n)\big), \end{aligned}$$

because $\varphi_{b_i}^{+} \circ \varphi_{b_i}$ is the identity map when restricted to $\mathbb{N}_0$. Note from Remark 2.3 that φ_{b_i} gives a bijection between $\mathbb{N}_0$ and the set R_{b_i} of rational numbers in $[0,1)$ with denominator a power of b_i. Further, $\varphi_{b_i}(0) = 0$. Therefore the equivalence of (i) and (ii) follows from (3) and the Weyl criterion in Lemma 3.2.

(ii) $\Leftrightarrow$ (iii). The implication (ii) $\Rightarrow$ (iii) is trivial. For the converse, we note that if $g_1, \dots, g_s \in \mathbb{N}_0$ not all 0 are given and we put $g = \max(g_1, \dots, g_s)$, then $b_1^g\mathbb{Z} \times \cdots \times b_s^g\mathbb{Z}$ is a subgroup of $b_1^{g_1}\mathbb{Z} \times \cdots \times b_s^{g_s}\mathbb{Z}$, and so uniform distribution mod $(b_1^g, \dots, b_s^g)$ implies uniform distribution mod $(b_1^{g_1}, \dots, b_s^{g_s})$.

(i) $\Leftrightarrow$ (iv). From the proof of the equivalence (i) $\Leftrightarrow$ (ii) above, it follows that

$$\text{(i)} \Leftrightarrow \lim_{N\to\infty} S_N\big(\chi_{\mathbf{k}}, (\mathbf{f}(n))_{n\geq 0}\big) = 0,$$

for all $\mathbf{k} \in \mathbb{N}_0^s$ with $\mathbf{k} \neq \mathbf{0}$. From the Weyl criterion in the compact abelian group $\mathbb{Z}_{\mathbf{b}}$ (see Kuipers and Niederreiter [8, Corollary 1.2, p. 227]), it follows that $\big(\mathbf{f}(n)\big)_{n\geq 0}$ is uniformly distributed in $\mathbb{Z}_{\mathbf{b}}$, and vice versa. □

Corollary 4.3. *Let $b_1 = \cdots = b_s =: p$, p prime. Then the following properties are equivalent:*

(i) *the sequence $(\mathbf{x}_n)_{n\geq 0}$ of points in (4) is uniformly distributed in $[0,1)^s$;*

(ii) *the sequence $\big(a_1 f_1(n)+\cdots+a_s f_s(n)\big)_{n\geq 0}$ of integers is uniformly distributed mod p^g for all $g \in \mathbb{N}$ and for all $(a_1,\dots,a_s) \in \mathbb{Z}^s$ with at least one a_i coprime to p.*

Proof. It suffices to show that property (ii) in Corollary 4.3 is equivalent to property (iii) in Theorem 4.2. First assume that property (ii) in Corollary 4.3 holds. Now choose $g \in \mathbb{N}$. In order to prove that $\big((f_1(n),\dots,f_s(n))\big)_{n\geq 0}$ is uniformly distributed mod $(p^g,\dots,p^g)$, we need to show according to Lemma 3.2 that for all $(h_1,\dots,h_s) \in \{0,1,\dots,p^g-1\}^s \setminus \{\mathbf{0}\}$ we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{h_1}{p^g} f_1(n) + \cdots + \frac{h_s}{p^g} f_s(n)\right) = 0. \tag{5}$$

Put $p^d = \gcd(h_1,\dots,h_s,p^g)$ and note that $d < g$. We can write $h_i = a_i p^d$ with $a_i \in \{0,1,\dots,p^{g-d}-1\}$ for $1 \leq i \leq s$ and at least one a_i coprime to p. Then (5) follows from the fact that

$$\big(a_1 f_1(n) + \cdots + a_s f_s(n)\big)_{n\geq 0}$$

is uniformly distributed mod p^{g-d}.

For the converse, choose $g \in \mathbb{N}$ and $(a_1,\dots,a_s) \in \mathbb{Z}^s$ with at least one a_i coprime to p. In order to prove that $\big(a_1 f_1(n) + \cdots + a_s f_s(n)\big)_{n\geq 0}$ is uniformly distributed mod p^g, we need to show according to Lemma 3.2 that for any $h \in \mathbb{Z}$ with $1 \leq h < p^g$ we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{h}{p^g}\big(a_1 f_1(n) + \cdots + a_s f_s(n)\big)\right) = 0. \tag{6}$$

Since $\gcd(a_i,p) = 1$ for at least one i, we have $ha_i \not\equiv 0 \pmod{p^g}$ for this value of i and all values of h under consideration. Therefore (6) holds by Theorem 4.2 (iii) and Lemma 3.2. □

Remark 4.4. There is no obvious analog of Corollary 4.3 for the case where $s \geq 2$ and $p_1, \ldots, p_s$ are distinct primes. Consider the sequence $(\mathbf{x}_n)_{n \geq 0}$ in (4) with $f_i(n) = n$ for all $1 \leq i \leq s$ and $n \geq 0$. Then the sequence

$$\big((f_1(n), \ldots, f_s(n))\big)_{n \geq 0} = \big((n, \ldots, n)\big)_{n \geq 0}$$

is uniformly distributed mod $(p_1^g, \ldots, p_s^g)$ for all $g \in \mathbb{N}$ by the Chinese remainder theorem (see also Corollary 2.18), and so the sequence $(\mathbf{x}_n)_{n \geq 0}$ is uniformly distributed in $[0,1)^s$ by Theorem 4.2. On the other hand, take any integers $a_1, \ldots, a_s$ with $a_1 + \cdots + a_s = 0$. Then there is no modulus $m \geq 2$ for which the sequence

$$\big(a_1 f_1(n) + \cdots + a_s f_s(n)\big)_{n \geq 0} = \big((a_1 + \cdots + a_s)n\big)_{n \geq 0}$$

is uniformly distributed mod m.

5. Some constructions

Example 5.1. Let $(F_n)_{n \geq 0}$ be the Fibonacci sequence. It was shown in Niederreiter [12] that $(F_n)_{n \geq 0}$ is uniformly distributed mod 5^g for all $g \in \mathbb{N}$. It follows therefore from Theorem 4.2 that the sequence $\big(\varphi_5(F_n)\big)_{n \geq 0}$ is uniformly distributed in $[0,1)$.

Remark 5.2. Note that $(F_n)_{n \geq 0}$ is a second-order linear recurring sequence. We could consider two second-order linear recurring sequences $(u_n)_{n \geq 0}$ and $(v_n)_{n \geq 0}$ of nonnegative integers satisfying the same linear recurrence relation modulo a prime p and then for $s = 2$ try $f_1(n) = u_n$ and $f_2(n) = v_n$ for all $n \geq 0$. But then we claim that the sequence $\big((f_1(n), f_2(n))\big)_{n \geq 0}$ is not uniformly distributed mod (p^g, p^g) for all $g \in \mathbb{N}$. To prove this claim, we note that it is a necessary condition that $(u_n)_{n \geq 0}$ be uniformly distributed mod p. Then by [15, Cor. 3] the minimal polynomial $m(x) \in \mathbb{F}_p[x]$ of $(u_n)_{n \geq 0}$ mod p has multiple roots, hence it is of the form $m(x) = (x - c)^2$ for some $c \in \mathbb{F}_p$. The generating functions mod p of $(u_n)_{n \geq 0}$ and $(v_n)_{n \geq 0}$, respectively, in the sense of [9, Sect. 6] are then of the form

$$\frac{l_1(x)}{(x-c)^2}, \quad \frac{l_2(x)}{(x-c)^2},$$

with polynomials $l_1, l_2 \in \mathbb{F}_p[x]$, $\deg(l_j) \leq 1$ for $j = 1, 2$, and $l_1(c) \neq 0$ (see [9, Thm. 6.2]).

Now choose $a_2 = 1 \in \mathbb{F}_p$ and $a_1 \in \mathbb{F}_p$ such that $a_1 l_1(c) + a_2 l_2(c) = 0$. Then the generating function mod p of $(a_1 u_n + a_2 v_n)_{n \geq 0}$ is given by

$$\frac{a_1 l_1(x) + a_2 l_2(x)}{(x-c)^2} = \frac{b}{x-c}$$

for some $b \in \mathbb{F}_p$. Therefore the minimal polynomial of $(a_1 u_n + a_2 v_n)_{n \geq 0}$ mod p is either 1 or $x - c$, hence it has no multiple roots, and so $(a_1 u_n + a_2 v_n)_{n \geq 0}$ is not uniformly distributed mod p. Thus, the property (ii) in Corollary 4.3 does not hold.

Example 5.3. Let $\alpha_1, \ldots, \alpha_s$ be positive real numbers such that $1, \alpha_1, \ldots, \alpha_s$ are linearly independent over $\mathbb{Q}$ and let $b_1, \ldots, b_s$ be arbitrary integers ≥ 2. Then for any $g \in \mathbb{N}$, the sequence

$$\Big(\big(\{n\alpha_1/b_1^g\}, \ldots, \{n\alpha_s/b_s^g\}\big)\Big)_{n \geq 0}$$

is uniformly distributed in $[0,1)^s$, and so by Lemma 3.3 the sequence

$$\Big(\big(\lfloor n\alpha_1 \rfloor, \ldots, \lfloor n\alpha_s \rfloor\big)\Big)_{n \geq 0}$$

is uniformly distributed mod $(b_1^g, \ldots, b_s^g)$. Thus, if we put $f_i(n) = \lfloor n\alpha_i \rfloor$ for $1 \leq i \leq s$ and $n \geq 0$, then the sequence of points in (4) is uniformly distributed in $[0,1)^s$ according to Theorem 4.2. We can also choose positive real numbers $\alpha_1, \ldots, \alpha_s$ in such a way that $\alpha_1 = 1/d$ for some $d \in \mathbb{N}$ and $1, \alpha_2, \ldots, \alpha_s$ are linearly independent over $\mathbb{Q}$. Then by [13, Theorem 2.7] the sequence

$$\Big(\big(\lfloor n\alpha_1 \rfloor, \ldots, \lfloor n\alpha_s \rfloor\big)\Big)_{n \geq 0}$$

is uniformly distributed mod $(b_1^g, \ldots, b_s^g)$ for all $g \in \mathbb{N}$, and so we can again take $f_i(n) = \lfloor n\alpha_i \rfloor$ for $1 \leq i \leq s$ and $n \geq 0$ and conclude that the sequence of points in (4) is uniformly distributed in $[0,1)^s$.

Example 5.4. Let $d_1, \ldots, d_s$ be distinct positive integers and let $\alpha_1, \ldots, \alpha_s$ be positive irrational numbers. Then for any integers $b_1, \ldots, b_s \geq 2$ and any $g \in \mathbb{N}$, the sequence

$$\Big(\big(\{\alpha_1 n^{d_1}/b_1^g\}, \ldots, \{\alpha_s n^{d_s}/b_s^g\}\big)\Big)_{n \geq 0}$$

is uniformly distributed in $[0,1)^s$, and so we see as in Example 5.3 that we can take $f_i(n) = \lfloor \alpha_i n^{d_i} \rfloor$ for $1 \leq i \leq s$ and $n \geq 0$ to obtain a sequence of points in (4) which is uniformly distributed in $[0,1)^s$.

Acknowledgements. The first author would like to thank Pierre Liardet, CMI, Université de Provence, Marseille, France, for his hospitality during the research visit where parts of this paper were written.

REFERENCES

[1] BEER, S.: *Zur Theorie der Gleichverteilung im p-adischen*, Österreich. Akad. Wiss. Math.-Natur. Kl. S.-B. II **176** (1967/1968), 499–519.

[2] DICK, J. – PILLICHSHAMMER, F.: *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010.

[3] HELLEKALEK, P.: *General discrepancy estimates: the Walsh function system*, Acta Arith. **67** (1994), 209–218.

[4] HELLEKALEK, P.: *A general discrepancy estimate based on p-adic arithmetics*, Acta Arith. **139** (2009), 117–129.

[5] HELLEKALEK, P.: *A notion of diaphony based on p-adic arithmetic*, Acta Arith. **145** (2010), 273–284.

[6] HEWITT, E. – ROSS, K. A.: *Abstract Harmonic Analysis. Vol. I, Structure of Topological Groups, Integration Theory, Group Representations.* (Second ed.), *Grundlehren der Mathematischen Wissenschaften* [Fundamental Principles of Mathematical Sciences] **115**, Springer-Verlag, Berlin, 1979.

[7] HOFER, R. – KRITZER, P. – LARCHER, G. – PILLICHSHAMMER, F.: *Distribution properties of generalized van der Corput-Halton sequences and their subsequences*, Int. J. Number Theory, **5** (2009), 719–746.

[8] KUIPERS, L. – NIEDERREITER, H.: *Uniform Distribution of Sequences*, John Wiley, New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.

[9] LIDL, R. – NIEDERREITER, H.: *Finite fields and their applications*, (M. Hazewinkel, ed.), in: *Handbook of Algebra*, Vol. 1, North-Holland, Amsterdam, 1996, pp. 321–363.

[10] MAHLER, K.: *Lectures on Diophantine Approximations. Part I: g-adic Numbers and Roth's Theorem*, University of Notre Dame Press, Notre Dame, 1961.

[11] MEIJER, H.G.: *Uniform distribution of g-adic integers*, Nederl. Akad. Wetensch. Proc. Ser. A **70** = Indag. Math., **29** (1967), 535–546.

[12] NIEDERREITER, H.: *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quart., **10** (1972), 373–374.

[13] NIEDERREITER, H.: *On a class of sequences of lattice points*, J. Number Theory, **4** (1972), 477–502.

[14] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[15] NIEDERREITER, H. – SHIUE, J.-S.: *Equidistribution of linear recurring sequences in finite fields*, Nederl. Akad. Wetensch. Proc. Ser. A **80** = Indag. Math., **39** (1977), 397–405.

[16] SLOAN, I.H. – JOE, S.: *Lattice Methods for Multiple Integration*, Clarendon Press, Oxford, 1994.

Received January 26, 2011
Accepted March 20, 2011

Peter Hellekalek
Dept. of Mathematics
University of Salzburg
Hellbrunnerstrasse 34
5020 Salzburg
AUSTRIA
E-mail: peter.hellekalek@sbg.ac.at

Harald Niederreiter
Johann Radon Institute for
Computational and
Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
4040 Linz
AUSTRIA

Dept. of Mathematics and
Statistics
King Fahd University
of Petroleum & Minerals
P.O. Box 5046
Dhahran 31261
SAUDI ARABIA
E-mail: ghnied@gmail.com